DEPARTMENT OF THE ARMY
79th Ordnance Battalion (EOD)
52d Ordnance Group (EOD)
Fort Sam Houston, Texas 78234-5056

AFOD-B (1oo) 11 July 2001

MEMORADUM FOR SEE DISTRIBUTION

SUBJECT: Supplement to OI 380-19, Information Systems Security

1. REFERENCE: AR 380-19, Information System Security.

2. PURPOSE: Supplement policies and procedures as set forth in 52d Ordnance Group (EOD) Operating Instruction (OI) 380-19, Automation Security.

3. SCOPE: This supplement is directive in nature and is applicable to all personnel assigned or attached for duty with the 79th Ordnance Battalion (EOD) and it's subordinate units.

4. Add the following subparagraphs to paragraph 5:

a. Subparagraph g: The Company Commander is responsible for his / her companies Automation Security Program and is designated as the Information Systems Security Officer (ISSO) under the supervision of the ISSM and will perform those duties specified in AR 380-19, paragraph 3-6d(3).

b. Subparagraph h: All company personnel will protect the Automated Data Processing (ADP) resources within their control. Personnel will comply with the provisions of this OI and the cited references, correct all violations immediately and report them to the ISSO.

c. Subparagraph i: All computers will have a sensitivity designation IAW AR 380-19, paragraph 2-2a. The highest level authorized at this time is Critically Sensitive Level 3. Prior to processing classified material, a computer system must be accredited by the local installation accreditation authority and must be IAW AR 380-19, Chapter 3. However, the Facility Security Profile (FSP) and accreditation documentation may be modified to accommodate small laptop computers.

d. Subparagraph j: Small computers designated as "Highly Sensitive" or lower, will have the documentation with the rationale stating why accreditation is not necessary and signed by the individual who would have been the accreditation authority.

e. Subparagraph k: When required by local authorities, place a label on the computer system indicating the highest level of information that may be processed on that system.

f. Subparagraph l: Accreditation requires triennial updating unless certain system changes occur sooner as outlined in AR 380-19, paragraph 3-6a.

g. Subparagraph m: The ISSO will periodically check for proper and authorized usage as well as appropriate information security procedures.

h. Subparagraph n: All personnel will receive a briefing outlining the importance of the individual's security responsibilities. This briefing will also cover the local security environment and computer/hardware. Minimum requirements of this briefing are outlined in AR 380-19, paragraph 2-16a. This briefing will be documented and filed in the unit security files. Newly assigned personnel will be given an initial automation security and awareness training before they are authorized to use unit ADP systems. Personnel not assigned to the unit will not be authorized to process classified or sensitive data on unit ADP systems. The ISSO will conduct periodic security training and awareness classes. Records of these briefings and training will be maintained in the unit training files.

i. Subparagraph o: Units will store, control, and account for commercially procured software as durable items using hand receipt procedures IAW DA Pam 710-2-1. The ISSO will inventory these programs as least one time annually. Results of these inventories will be maintained in the unit supply files.

5. Efficient and Effective!

PATRICK J. KELLY
LTC, OD
Commanding

DISTRIBUTION:
A